IN THE CLAIMS

Please amend the claims as follows.

1. (Previously Presented) A method of securing digital content on a hard drive of computer, comprising:

providing a physical key adapted to be carried by a user;

detecting the physical key with a receiver/decoder circuit communicating with the hard drive;

validating the detected physical key with the receiver/decoder circuit wherein validating includes determining whether or not the detected physical key is associated with the hard drive; and

permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected key is validated wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the detected physical key in order to provide sector-level protection.

2. (Original) The method of claim 1, wherein the receiver/decoder circuit resides in the computer.

3. (Original) The method of claim 1, wherein the detecting step includes detecting the key over a secure wireless link.

4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein the receiver/decoder circuit enables the hard drive if the detected key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

6. (Previously Presented) The method of claim 5, wherein digital content stored on the drive is not encrypted with the key.

7. (Canceled)

8. (Previously Presented) The method of claim 1, wherein the key associated with the hard drive is initially delivered with the hard drive.

9. (Previously Presented) A system for securing digital content on a hard drive of a computer, comprising:

a physical key adapted to be carried by a user;

a hard drive having digital content; and

a receiver/decoder circuit communicating with the hard drive for detecting and validating the physical key wherein the receiver/decoder circuit validates the physical key by determining whether or not the detected physical key is associated with the hard drive wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the hard drive using the physical key associated with the hard drive in order to provide sector-level protection.

10. (Original) The system of claim 9, wherein the receiver/decoder circuit resides in the computer.

11. (Original) The system of claim 9, wherein the receiver/decoder circuit detects the key over a secure wireless link.

12. (Canceled)

13. (Previously Presented) The system of claim 9, wherein the receiver/decoder circuit enables the hard drive if the detected physical key is validated and disables the hard drive if the detected

key is not validated in order to provide hard drive level protection.

14. (Previously Presented) The system of claim 9, wherein digital content stored on the computer is not encrypted with the physical key.

15. (Canceled)

16. (Previously Presented) The system of claim 9, wherein the physical key associated with the hard drive is initially delivered with the hard drive.

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

[[26]]27. (Currently Amended) The method of claim 1 wherein each sector is encrypted or decrypted by receiver/decoder circuit using the personal digital key associated with a drive corresponding to the sector.

[[27]] 28. (Currently Amended) The method of claim 1 wherein the sector level protection includes individual data sectors and clusters of data sectors.

[[28]] 29. (Canceled)

[[29]] 30. (Canceled)

[[30]] 31. (Currently Amended) [The] A method [of claim 29] of securing a hard drive of a computer, comprising: providing a portable, physical key adapted to be carried by a user, wirelessly detecting the portable, physical key with a receiver/decoder circuit communicating with the hard drive when the key is in proximity to the receiver/decoder circuit; validating the detected portable physical key with the receiver/decoder circuit; and permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected portable physical key is validated wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive.

[[31]] 32. (Canceled)